



Department of Homeland Security Daily Open Source Infrastructure Report for 30 August 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- AEP Ohio has issued a warning to copper wire thieves saying that their safety is at risk; at least four people have been electrocuted during attempted thefts brought on by a rise in scrap metal prices. (See item [1](#))
- Platts Energy Bulletin reports the Coast Guard has closed the ports of Miami, Port Everglades, and Key West to all inbound and outbound shipping traffic as of 8 a.m. EDT Tuesday, August 29, as Tropical Storm Ernesto heads towards Florida. (See item [17](#))
- The New York Times reports scientists have developed a detailed influenza test that takes less than 12 hours; this new technology, a microchip covered with bits of genetic material from many different flu strains, cuts the time needed for diagnosis of the H5N1 flu to less than a day. (See item [30](#))
- The Department of Homeland Security's Federal Emergency Management Agency is ready and supporting state officials as they prepare for Tropical Storm Ernesto; the Agency continues to monitor the storm with the National Hurricane Center. (See item [34](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) –

1. *August 29, Times-Reporter (OH)* — **Would-be copper wire thieves could be in for a fatal shock.** AEP Ohio has issued a warning to thieves, amid a jump in thefts of copper wire fueled by a rise in scrap metal prices. While service outages and repair costs certainly disrupt the power company's business, company officials are emphasizing public safety. AEP Ohio has documented 46 break-ins at power substations in Ohio, including one in Tuscarawas County. Shelly DiMattio, a communication consultant in the AEP Ohio Canton office, also pointed out that's only the documented cases and unconfirmed break-ins could push that number higher. AEP substations are protected by barbed-wire fences for good reason. DiMattio described the current levels pulsing through the units as "absolutely deadly." An AEP Ohio press release mentions three people in Kentucky and Virginia who were electrocuted during attempted thefts and a British Columbia man who died from contact with a high voltage line while trying to strip metal from a substation. To combat theft, AEP has a toll-free, 24-hour hotline dedicated to security issues at (888) 747-5845. Additionally, the company is working with law enforcement and scrap dealers to curtail the thefts. DiMattio said AEP has asked dealers to ask scrap sellers for identification and contact information of resellers.
Source: <http://www.timesreporter.com/index.php?ID=57798&r=4>
2. *August 29, Hutchinson News (KS)* — **Wire theft causes electrical overload.** Some thieves will stop at nothing to pull the electricity conducting metal from some of the places it resides, such as cooling coils of large commercial air conditioning units or wiring from city street lights. Sometime between Saturday evening and Sunday afternoon, August 26-27, one or more malicious recyclers cut large pieces of 3/4-inch copper wire from a series of "live" electrical panels behind the New Beginnings building in Hutchinson, KS. The damage left the building without power. The thievery, the second of its kind in less than a year at the building, nearly started an electrical fire. Inside the well-hidden, large electrical panels, the thieves severed the neutral wires while leaving the "hot" wires in place. The result was an electrical circuit that bypassed the emergency breakers and loaded low-voltage wires with immense heat as the current sought to replace the severed grounding wire. Hutchinson Police detective Thad Pickard said he's noticed an increase in copper thefts since March, when copper peaked at nearly \$4 per pound. Pickard said, "We've had window air conditioners stolen, and the coils taken out of commercial units."
Source: <http://www.hutchnews.com/news/local/stories/theft082906.shtm>
3. *August 28, Associated Press* — **AES constructs Texas-based wind farm.** Global power producer AES Corp. said Monday, August 28, it has started building a wind farm near Abilene, TX, and has signed a 10-year power purchase agreement to sell all of the electricity the project produces to Texas electric provider Direct Energy. AES said the project expands on an existing wind farm in the area, making it the largest operating wind farms in the U.S. by generating enough energy to power about 100,000 homes in Texas.
Source: http://biz.yahoo.com/ap/060828/aes_contract.html?.v=1

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

4. *August 29, Detroit News* — **Chemical plant fire prompts evacuation of near by residents.** A fire Monday, August 28, at the Petro–Chem Processing Inc. in Detroit, MI, prompted the evacuation of residents within a half–mile radius of the plant at Lycaste and Freud. Fire officials said the evacuation was not massive because of the time of day and some residents stayed in their homes and kept their windows shut. The fire began in an area where aerosol cans are prepared for disposal.
Source: <http://www.detnews.com/apps/pbcs.dll/article?AID=/20060829/METRO/608290335>
5. *August 29, Atlanta Journal–Constitution* — **Truck spills sulfuric acid in Georgia.** A chemical spill shut down the main street through downtown Austell, GA, during the Tuesday, August 29, morning commute. A dump truck overturned at C&S Chemicals on Railroad Avenue, knocking a hole in a tank of sulfuric acid. About 200 gallons of the acid spilled from the tank. Although, the acid was contained to company property, a two–block stretch of Veterans Memorial Highway was closed and traffic was diverted onto Jefferson Street.
Source: http://www.ajc.com/metro/content/metro/cobb/stories/0829mets_pill.html
6. *August 28, Tribune–Democrat (PA)* — **Vandals spill 1,500 gallons of diesel fuel.** Cleanup crews spent Monday, August 28, vacuuming more than 1,500 gallons of off–road diesel fuel at a Bakersville, PA, construction company in what company officials called the most extreme act in a spate of vandalism there. Someone released the fuel as well as 200 gallons of gear oil from tanks on New Enterprise Stone & Lime Co. property in Jefferson Township. Perpetrators drilled a 1/4–inch diameter hole into the fuel tank and opened a valve on a gear oil tank.
Source: http://www.tribune-democrat.com/local/local_story_240230446.html?keyword=secondarystory
7. *August 28, Indiana Daily Student* — **Fire crews evacuate center of Indiana campus after gas leak.** Indiana firefighters and police blocked access to much of the center of campus late Sunday night and early Monday, August 28, after Indiana University employees reported a hydrogen chloride gas leak in the chemistry building. Police evacuated multiple buildings and would not let passers by within 330 feet of the site as Hazmat crews entered the building and removed a leaking gas cylinder.
Source: <http://www.idsnews.com/news/story.php?id=36978&adid=campus>

[\[Return to top\]](#)

Defense Industrial Base Sector

8. *August 28, U.S. Joint Forces Command* — **Joint Systems Baseline Assessment 2006 prepares for operational stage.** U.S. Joint Forces Command's Joint Systems Integration Command (JSIC) is preparing for the second phase of the Joint Systems Baseline Assessment 2006 (JSBA–06) to be held September 5–28 at JSIC's labs and other sites linked in to the effort from around the world. The purpose of JSBA–06 is to identify and address warfighter interoperability issues relating to capabilities already in the field or projected to be in the field in the next year. Successful resolution of these issues will allow warfighters to more effectively use and share information. JSBA–06 kicked off in July with the two–week technical assessment, where warfighters, program managers, and engineers worked on evaluating more

than 30 joint task force command and control systems of record in a controlled environment.
The second phase of JSBA-06 is the operational assessment.

Source: <http://www.jfcom.mil/newslink/storyarchive/2006/pa082806.htm>

[[Return to top](#)]

Banking and Finance Sector

9. *August 29, Associated Press* — **Banks severing ties with North Korea.** The financial noose is around North Korea as international banks sever ties with the nation — a move championed by the United States, a top Department of the Treasury official said. The United States has accused Pyongyang of spreading weapons and missile technology to other countries, counterfeiting U.S. currency and trafficking drugs. It wants to see the reclusive, communist-led regime financially incapacitated. "There is sort of a voluntary coalition of financial institutions saying that they don't want to handle this business anymore and that is causing financial isolation for the government of North Korea," Stuart Levey, the Department of the Treasury's undersecretary for terrorism and financial intelligence, said in an interview Monday, August 28, with The Associated Press. In other matters, Levey called Iran a "central banker of terror" that provides millions of dollars a year to bankroll terrorist acts carried out by the militant group Hezbollah.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/29/AR2006082900164.html>

10. *August 28, Associated Press* — **T-Mobile hacker gets home detention.** A hacker who infiltrated the network of T-Mobile USA Inc. and accessed personal information of hundreds of customers, including a Secret Service agent, was sentenced Monday, August 28, to one year of home detention. Nicholas Lee Jacobsen, 23, must also pay \$10,000 in restitution to T-Mobile to cover losses caused by his acts, which took place in 2004. When Jacobsen targeted the network of T-Mobile USA, he uncovered the names and Social Security numbers of 400 customers. Jacobsen was also able to read some sensitive information that Special Agent Peter Cavicchia could access through his wireless T-Mobile Sidekick device. No investigations were compromised, the Secret Service said.

Source: http://news.yahoo.com/s/ap/20060829/ap_on_hi_te/cellular_hac_ker

11. *August 28, Websense Security Labs* — **Multiple phishing alert: Caixa Geral de Depositos, Service Credit Union.** Websense Security Labs has received reports of several new phishing attacks. One attack targets Caixa Geral de Depositos in Portugal. Users receive a spoofed e-mail message claiming that a new investigation on money laundering requires a verification of all account details. The URL provided in the e-mail is a link to a phishing site that attempts to collect users' account information, such as login details. Another attack targets Service Credit Union. Users receive a spoofed e-mail message claiming that a new security system is being implemented, so account details need to be confirmed in order to activate the new security features. The e-mail provides a link to a phishing site that attempts to collect the user's account information.

Screen shots:

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=589>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=590>

Source: <http://www.websense.com/securitylabs/alerts/>

12. *August 25, OUT–LAW News (United Kingdom)* — **Australian citizen database subjected to snooping by government employees.** Australia's citizen database was routinely searched for personal reasons by government agency employees, some of whom have been fired. Police are now investigating allegations of identity fraud resulting from the security breaches. There were 790 security breaches at government agency Centrelink involving 600 staff. Staff were found to have inappropriately accessed databases containing citizens' information. The databases are used to administer social security, pension and unemployment benefits. Australian police have confirmed that investigations are ongoing after five referrals were made to it from Centrelink. At least one of the cases is believed to involve allegations of the establishment of fake identities to be used to receive payments.

Source: <http://www.out-law.com/page-7229>

13. *August 25, CNET News* — **Verizon gaffe lets customer details slip.** Verizon Wireless last week accidentally distributed a file with limited details on more than 5,000 customers outside the company, potentially giving identity thieves a toehold. The Microsoft Excel spreadsheet file was e-mailed on Monday, August 21, and includes names, e-mail addresses, cell phone numbers and cell phone models of 5,210 Verizon Wireless customers. All of the customers have Motorola Razr phones, according to the spreadsheet. The spreadsheet was inadvertently sent to about 1,800 people, all Verizon Wireless subscribers, according to a follow-up e-mail apologizing for the gaffe that the mobile carrier sent on Thursday, August 24. The Excel file was attached to an ad for a Bluetooth wireless headset, instead of the electronic order form that was supposed to be sent.

Source: http://news.com.com/Verizon+gaffe+lets+customer+details+slip/2100-1029_3-6109883.html

[[Return to top](#)]

Transportation and Border Security Sector

14. *August 29, USA TODAY* — **Fliers board faster with fewer carry-on bags.** In an unforeseen twist, new security rules for carry-on bags are enabling airline passengers to get on and off planes faster, helping flights leave on time. The reason: less on-board congestion from fewer carry-on bags stowed in overhead bins or under seats. US Airways is boarding planes five to 10 minutes faster, depending on the size of the plane and how crowded it is, says Senior Vice President Anthony Mulé. Following terror-related arrests in London, the Transportation Security Administration on August 10 banned liquids, creams, and gels from the plane's cabin. Airlines say they're handling up to 25 percent more checked bags now as travelers adjust to the rules. Airlines say they're struggling to deal with the huge surge in bags. Airline ticket agents, baggage tug drivers and bag handlers are racking up overtime. Carriers won't say exactly how much they're spending, but "it's expensive," says AirTran Airways spokesperson Tad Hutcheson. At Delta Air Lines, the increased bag volume is straining aging luggage systems at its main Atlanta hub and at New York John F. Kennedy Airport. If the new rules stay in place, Delta COO Jim Whitehurst says the airline soon will hire more baggage workers.

Source: http://www.usatoday.com/travel/flights/2006-08-29-bags-usat_x.htm

15.

August 29, Washington Post — **Seven dead in second Kentucky plane crash in two days.** A small plane carrying seven people crashed Monday, August 28, in a wooded, mountainous area of southeastern Kentucky, about 100 miles from the site of Sunday's commuter-jet crash in Lexington. The twin-engine Cessna departed from Kickapoo Downtown Airport near Wichita Falls, TX, said Kathleen Bergen, spokesperson for the Federal Aviation Administration in Atlanta. She said she didn't know the destination because the pilot did not file a flight plan. The crash site is so remote that rescue workers on all-terrain vehicles needed help from a helicopter to find it, said Buddy Rogers, a spokesperson for the Kentucky Division of Emergency Management. There was rain, thunder and light fog in the area for much of the afternoon, said Tom Johnstone, a meteorologist with the National Weather Service.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/28/AR2006082801529.html>

16. *August 29, Great Falls Tribune (ND)* — **Northern Border Air Wing increases security.** The Northern Border Air Wing — a division of Homeland Security Customs and Border Protection Air and Marine — will have its first aircraft for the new Great Falls, ND, post in place on Wednesday, August 30. This is the third post of what will eventually be five dotting the U.S.–Canada border. Posts in Washington and New York are operational and the other two will open in North Dakota and Michigan next year. The wing gives northern border protection efforts new tools to chase down criminals and prevent terrorists from entering the United States. Pilots and crews are trained and equipped to not only spot suspicious planes, but also to chase them down. Customs and Border Protection Air and Marine already is in place at the nation's southern border and coasts. Congress approved funds to extend their services to America's northern border after the September 11, 2001 terrorist attacks. The new post means increased activity at the Great Falls International Airport.

Source: <http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20060829/NEWS01/608290303/1002>

17. *August 29, Platts Energy Bulletin* — **Coast Guard closes Miami, Port Everglades, Key West for Ernesto.** The Coast Guard has closed the ports of Miami, Port Everglades, and Key West to all inbound and outbound shipping traffic as of 8 a.m. EDT Tuesday, August 29, as Tropical Storm Ernesto heads towards Florida, a spokesperson for the Coast Guard said. The center of the storm is expected to sweep through the Florida Keys or southeast Florida by Tuesday evening, according to the U.S. National Hurricane Center. Key West had suspended shipping traffic Monday evening, Coast Guard Petty Officer Dana Warr said. Fuel trucks were allowed to operate as normal inside the ports of Miami and Port Everglades, but all ship movement has stopped, he said. It was not known when the ports would reopen but generally, once the storm passes, a survey is conducted to determine when ports would be able to reopen.

Source: <http://www.platts.com/HOME/News/7677168.xml?sub=HOME&p=HOME/News&?undefined&undefined>

18. *August 29, Reuters* — **Morocco raises airport security on militant threat.** Morocco has stepped up security at its airports after discovering that the wives of two pilots at national airline Royal Air Maroc (RAM) had been funding a radical Islamist cell, state news agency MAP reported. "The Interior Ministry revealed on Tuesday (August 29), the proven implication of three Moroccan women, two of them married to RAM pilots, in the terrorist enterprise led by the Ansar El Mehdi cell recently dismantled by the security services," MAP said. The

government said earlier this month it had broken up a militant network that was planning to declare a holy war in the northeast of the country. The authorities arrested over 40 members of the previously unknown Jammaat Ansar El Mehdi (El Mehdi Support Group) and seized explosives, propaganda material and laboratory equipment.

Source: <http://www.alertnet.org/thenews/newsdesk/B242391.htm>

19. *August 28, Arizona Republic* — **Airport security boosts charter jets' business.** Interest in business charters, which spiked following September 11, 2001, is under the aviation spotlight once again since the August 10 ban on liquids, gels, and creams aboard commercial airline flights. Charter companies across the country have reported an increase in sales and inquiries since this latest security measure. The Transportation Security Administration (TSA) mandates specific guidelines for aircraft between 12,500 and 100,000 pounds, which includes most charter jets. But these security measures focus more on advance screening of individuals rather than the metal detector type mass scrutiny directed at commercial travelers. "We work very closely with the 17 associations that make up the General Aviation Coalition to ensure security mandates are based on threat analysis and risk management, balanced with common sense," said Jennifer Marty-Peppin, a Western regional TSA spokesperson. Yet, another group of charters require virtually no security. These are propeller driven aircraft under 12,500 pounds that generally service the leisure market and commonly make small trips from the Valley to popular markets like Las Vegas or the Grand Canyon. Critics argue that these scheduled-service charters are particularly vulnerable to terrorists because they need no security and their flights are advertised in advance.

Source: <http://www.azcentral.com/news/articles/0828biz-charter-ON.htm>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

20. *August 29, Western Farm Press* — **Tomato virus spreading.** Tomato spotted wilt virus (TSWV) in tomatoes has been increasing, both in the southern San Joaquin Valley as well as in San Joaquin County, CA, according to Brenna Aegerter, vegetable farm advisor for the county. TSWV has an extremely wide host range, including hundreds of plants species spanning both broadleaves and monocots like as orchids and lilies. Economic hosts in California include tomato, pepper, beans, corn, lettuce, radicchio, celery and many ornamentals. Plant pathologists from University of California–Davis are currently studying the outbreaks in tomatoes in conjunction with Cooperative Extension Farm Advisors who are looking for fields with high incidents of wilt.

TSWV information: <http://vegetablemdonline.ppath.cornell.edu/factsheets/VirusSpottedWilt.htm>

Source: <http://westernfarmpress.com/news/08-29-tomato-spot-virus/>

21. *August 29, Animal and Plant Health Inspection Service* — **Import restrictions on live fish, fertilized eggs and gametes.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is proposing to establish regulations restricting the importation of live fish, fertilized eggs and gametes of fish from certain species that are susceptible to spring viremia of carp (SVC). The following species are considered susceptible to SVC: common carp (including koi), grass carp, silver carp, bighead carp, Crucian carp, goldfish, tench and sheatfish. SVC is an extremely contagious viral disease of carp. Outbreaks of SVC confirmed in the U.S. in 2002 and 2004, and since eradicated, have been linked to unregulated importation of SVC-infected fish. This action is necessary to prevent further introductions of the virus into the U.S. This action becomes effective September 29.

Source: <http://www.aphis.usda.gov/newsroom/content/2006/08/svcrestri c.shtml>

22. *August 28, U.S. Department of Agriculture* — **Avian influenza tests complete on Michigan mute swans.** The U.S. Department of Agriculture (USDA) Monday, August 28, announced final test results, which confirm that an H5N1 avian influenza virus detected in samples collected earlier this month from two Michigan wild mute swans is a low pathogenic subtype. The USDA National Veterinary Services Laboratories (NVSL) confirmed the presence of the "North American strain" of low pathogenic H5N1 avian influenza in one of twenty samples collected from the two wild mute swans.

Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentonly=true&contentid=2006/08/0324.xml

[[Return to top](#)]

Food Sector

23. *August 29, USAgNet* — **Switzerland plans to block U.S. beef imports.** Consumers in Switzerland may find their grocery store's meat case lacking U.S. beef next year thanks to efforts by the Swiss government to more closely match the country's veterinary rules with those of the European Union. Switzerland is not a member of the European Union, preferring to remain politically neutral. The European Union closed its markets to U.S. beef. The European Union contends that U.S. beef is unsafe because some U.S. ranchers implant their cattle with growth-enhancing hormones. Switzerland allows the importation of U.S. beef, provided that all products from cattle treated with hormones are declared as such and hormone residues are no longer traceable.

Source: <http://www.usagnet.com/story-national.php?Id=1735&yr=2006>

24. *August 29, Agence France-Presse* — **Japanese restaurant chain starts serving U.S. beef again.** U.S. beef is back on the menu at Japanese barbecue restaurant Zenshoku, believed to be the first major chain to start serving the dish again after an import ban was lifted in July. Osaka-based Zenshoku will begin offering U.S. beef dishes at 57 of its restaurants in the Tokyo and Osaka area, alongside meat from other countries such as Japan and Australia, said Zenshoku spokesperson Hiroyuki Toriyama. Japan, formerly the top market for U.S. beef, had halted U.S. beef imports twice since December 2003 due to mad cow health scares. Beef bowl chain restaurant Yoshinoya has said that it is preparing to put U.S. beef back on the menu from late September.

Source: http://news.yahoo.com/s/afp/20060829/hl_afp/japanusbeefhealt

[[Return to top](#)]

Water Sector

25. *August 29, Los Angeles Times* — Proposed limit for perchlorate in drinking water.

Perchlorate, an ingredient of solid rocket fuel that is contaminating hundreds of wells throughout Southern California, would be limited in drinking water under a new state standard proposed Monday, August 28. The California Department of Health Services plans to set a drinking water standard of six parts per billion, the same as a goal the state established two years ago. The standard, however, would be enforceable, whereas the existing goal is not.

Source: <http://www.latimes.com/news/local/la-me-perchlorate29aug29.04030059.story?coll=la-home-local>

26. *August 28, United Press International* — Fish check water safety in San Francisco. The San Francisco Public Utilities Commission says the city has begun using common bluegill fish to guard against terror attacks on the water system. Commission General Manager Susan Leal said San Francisco and New York have become the first cities to use the process, which uses non-contact sensors placed in the aquarium, which is hooked into the water system, to monitor the fish's behavior and watch for indicators of toxic conditions. If toxins are suspected, the system triggers an alarm, takes water samples for analysis, and notifies staff 72 hours before the water reaches the public.

Source: <http://www.upi.com/NewsTrack/view.php?StoryID=20060828-081938-4044r>

27. *August 26, Associated Press* — Nuclear plants leak tritium into groundwater. The Tennessee Valley Authority's (TVA) three nuclear power plants have leaked a radioactive form of hydrogen called tritium into the groundwater, according to TVA documents and Nuclear Regulatory Commission (NRC) officials. The leaked tritium has not moved beyond TVA property and is not a public health hazard, NRC officials said. NRC spokesperson Kenneth Clark said if the leaked tritium reaches the Tennessee River, that body of water would dilute the substance until its concentration would not be a "health and safety issue for the public." Tritium is a byproduct created when electricity is produced with nuclear power. It is the least dangerous of radioactive materials. NRC inspector George Kuzo said groundwater sampling at all three Tennessee Valley Authority plants Watts Bar in Spring City, TN; Sequoyah in Soddy-Daisy, TN; and Browns Ferry in Athens, AL, revealed tritium, according to reports prepared by TVA for a nuclear industry trade group and shared with the NRC.

Source: <http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/15369793.htm>

28. *August 25, U.S. Food and Drug Administration* — Spring water recalled. Weis Markets Inc. on Friday, August 25, voluntarily recalled its one-gallon containers of Weis Quality Spring Water. The Company said it decided to recall its one-gallon containers after it received test results on the level of bromate in this product. The U.S. Food and Drug Administration allows 10 parts per billion as the maximum allowable level of bromate in bottled water. While some of the Company's tests showed no detectable levels of bromate, other tests indicated that levels exceeded the maximum level of ten parts per billion, with results ranging from zero to 19 parts

per billion.

Source: http://www.fda.gov/oc/po/firmrecalls/weiss08_06.html

[[Return to top](#)]

Public Health Sector

29. *August 29, Agence France–Presse* — Suspected human bird flu case admitted to

Indonesian hospital. A sixty-year-old man from Indonesia's West Java has been admitted to hospital on suspicion of having bird flu, a hospital official said. The man was sent to the general hospital in Garut, West Java from the hamlet of Cipicung in the isolated subdistrict of Cikelet where three people have already been infected by bird flu, said Yogi Suprayogi, the spokesperson of the hospital. The man who was admitted with high fever and respiratory problems — both symptoms of bird flu — owned 10 chicken which died suddenly two days before he went to the hospital, Suprayogi said. The district animal husbandry office has killed a total of 4,602 birds, including chicken, ducks, geese and doves in the six villages in Cikelet in the past days, said Dida, an official from the office in Garut.

Source: http://news.yahoo.com/s/afp/20060829/hl_afp/healthfluindonesia_060829064126

30. *August 29, New York Times* — New test speeds diagnosis of lethal avian flu strain. Scientists have developed a detailed influenza test that takes less than 12 hours. The new technology, a microchip covered with bits of genetic material from many different flu strains, cuts the typical time needed for diagnosis of the H5N1 flu to less than a day from a week or more. In addition, rather than giving just a yes-or-no result, it usually reveals which flu a human or an animal has. That means that public health officials investigating, for example, a flu outbreak in poultry or in humans in a remote Asian or African village will be able to decide quickly whether to kill thousands of birds or to treat hundreds of potentially exposed people with expensive antiviral drugs. Right now, ascertaining whether a flu is of the lethal A (H5N1) strain requires that a sample be frozen and shipped to a highly secure laboratory where the virus can be grown in eggs, isolated and genetically sequenced. That process takes four to five days plus shipping time. The new test can be performed in any laboratory that can amplify bits of genetic material; many countries have such laboratories in their national capitals, if not in provincial hospitals.

Source: http://www.nytimes.com/2006/08/29/health/29flu.html?_r=1&ref=us&oref=slogin

31. *August 28, Rensselaer Polytechnic Institute* — New anthrax inhibitor could combat antibiotic-resistant strains. In a new approach to treating anthrax exposure, a team of scientists, from Rensselaer Polytechnic Institute and the University of Toronto, has created an inhibitor designed to tackle the growing threat of antibiotic-resistant strains. Anthrax toxin, secreted by the anthrax bacterium, is made of proteins and toxic enzymes that bind together to inflict damage on a host organism. Rather than targeting the anthrax bacterium or toxin — the approach taken by the majority of current therapies — the new inhibitor blocks the receptors where anthrax toxin attaches in the body. The new approach led to a 50,000-fold increase in potency in cell culture, and the inhibitor protected rats from anthrax toxin in the study. The general concept also could be applied to designing inhibitors for other pathogens, the researchers note.

Source: [http://news.rpi.edu/update.do?artcenterkey=1697&setappvar=paged\(1\)](http://news.rpi.edu/update.do?artcenterkey=1697&setappvar=paged(1))

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

32. *August 29, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 am EDT the center of Tropical Storm Ernesto was located about 230 miles southeast of Key West, FL and about 235 miles south-southeast of Miami, FL. Ernesto is moving toward the northwest near 14 mph. On the forecast track Ernesto will be near the Florida Keys or southeast Florida by the evening of Tuesday, August 29. Maximum sustained winds are near 45 mph with higher gusts. Some strengthening is expected and Ernesto could be near Hurricane strength when it makes landfall along the southern Florida peninsula. Tropical storm force winds extend outward up to 85 miles from the center. Rainfall totals of five to 10 inches are possible over portions of eastern and southern Florida and the Keys through Wednesday, August 30. The Tropical Storm Warning is extended northward along the Florida east coast to New Smyrna Beach. A Tropical Storm Warning and a Hurricane Watch are now in effect from New Smyrna Beach southward on the east coast including lake Okeechobee from Bonita Beach southward on the west coast and for all of the Florida Keys from Ocean Reef to the Dry Tortugas.
To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>
Source: <http://www.fema.gov/emergency/reports/2006/nat082906.shtm>

33. *August 29, Boston Globe* — **Massachusetts terror drill will be gauge of readiness.** Less than a week after the fifth anniversary of the September 11, 2001 terrorist attacks, one of the largest anti-terror drills ever in New England will test how public safety officials deal with some of their worst fears — all at the same time. The scenario is scheduled to include an explosion in a lab, a threat to a natural gas facility, a dirty bomb inside a local mall, and the discovery of an improvised explosive device in a commuter train station. Operation Poseidon is scheduled for the morning of Sunday, September 17 and is sponsored by the Massachusetts Executive Office of Public Safety and Boston Mayor Thomas M. Menino's Office of Homeland Security. The exercise is designed to bring together federal, state, and local agencies, as well as hospitals and the National Guard, to coordinate and improve how they respond, communicate, and work together to tackle the fast-moving series of threats. "Operation Poseidon is an important test of our region's interoperable communications, emergency operations, and response capacity," Jennifer Mehigan, a spokesperson for Menino, said in a statement.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/08/29/drill_will_be_gauge_of_terror_readiness/

34. *August 28, Federal Emergency Management Agency* — **FEMA prepares for Tropical Storm Ernesto landfall.** The Department of Homeland Security's Federal Emergency Management

Agency (FEMA) is ready and supporting state officials as they prepare for Tropical Storm Ernesto, the fifth named storm of the 2006 hurricane season. FEMA continues to closely monitor the storm with the Hurricane Liaison Team at the National Hurricane Center and is coordinating with state and local officials as they make decisions for their communities on evacuations and response activities. FEMA preparations include: a) Engaging with governors and state emergency managers in the anticipated impact states to begin federal and state coordination; b) Working with partners at the National Hurricane Center to anticipate the storm's landfall; c) Mobilizing trucks with food, water and ice for the potentially affected areas; d) Activating FEMA's National Response Coordination Center in Washington, DC, and the Regional Response Coordination Center in Atlanta, GA, to Level 1, with a 24/7 operational period; e) Activating and deploying response teams to staging areas in Florida, Georgia and Alabama, including Federal Incident Response Support Teams, Disaster Medical Assistance Teams and Urban Search and Rescue Teams.

Source: <http://www.fema.gov/news/newsrelease.fema?id=29279>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

35. *August 29, Associated Press* — **Japan orders Apple to probe laptops.** Japanese authorities reported Tuesday, August 29, the first case of an Apple laptop catching fire in Japan and ordered the U.S. company to investigate the trouble involving the faulty Sony batteries and report back within a week. A laptop made by Apple Computer Inc. overheated and caught fire in April, the Ministry of Economy, Trade and Industry said. The user sustained minor burns after the iBook G4 computer caught fire. Apple has received nine reports in the United States of the lithium-ion battery packs overheating, including two consumers who received minor burns after handling overheated computers.

Source: http://news.yahoo.com/s/ap/20060829/ap_on_hi_te/japan_apple_battery_recall

36. *August 29, Sophos* — **Phony Apple iPod shipping notification e-mail leads to Trojan horse.** Sophos has warned of a Trojan horse that has been spammed out claiming to be a notification that an Apple iPod MP3 player has been shipped to them, and their account has been charged almost \$500. Sophos has received reports of the Troj/Dowdec-A Trojan horse, which arrives in a message claiming to be related to the purchase of an Apple iPod. The e-mails claim that the popular music player is being shipped via FedEx and that a payment of \$479.95 has been received from the recipient's e-gold account. Attached to the e-mails is a file called OrderInf.zip, which unpacks to OrderInfo.exe. Executing this file infects the user's computer with a Trojan horse that attempts to download further malicious code from the Internet. The Trojan horse only works on Windows computers, and cannot infect Apple Macs.

Source: http://www.sophos.com/pressoffice/news/articles/2006/08/ipod_email-trojan-horse.html

37. *August 28, Security Focus* — **Microsoft Windows Server Service remote buffer overflow vulnerability.** Microsoft Windows Server Service is prone to a remote buffer overflow vulnerability. This vulnerability arises when the service processes a malicious message in RPC communications. A successful attack may result in arbitrary code execution with system privileges leading to a full compromise. Attack attempts may result in denial-of-service

conditions as well. Microsoft has reported that this issue is being exploited in the wild. Update (August 14, 2006): A worm named "W32.Wargbot" that exploits this issue to spread is currently in the wild.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/19409/info>

Solution: Microsoft has released an advisory including fixes to address this issue. A Cisco advisory containing various mitigation strategies using Cisco products to prevent attacks is available. Please see the references for more information:

<http://www.securityfocus.com/bid/19409/references>

Source: <http://www.securityfocus.com/bid/19409/discuss>

38. *August 28, Security Focus* — **Mozilla Foundation Products XPCOM memory corruption vulnerability.** Various Mozilla Foundation products are prone to a memory corruption vulnerability. This issue occurs because the applications fail to handle simultaneous XPCOM events that would cause the deletion of the timer object. An attacker can exploit this issue to execute arbitrary code.

For a list of vulnerable products: <http://www.securityfocus.com/bid/19197/info>

Solution: New versions of Firefox, SeaMonkey, Camino, and Thunderbird are available to address this issue. Most Mozilla applications have self-updating features that may be used to download and install fixes. Please see the referenced advisories for information on obtaining and applying fixes: <http://www.securityfocus.com/bid/19197/references>

Source: <http://www.securityfocus.com/bid/19197/discuss>

39. *August 28, Security Focus* — **Microsoft Internet Explorer COM object instantiation daxctl.OCX heap buffer overflow vulnerability.** Microsoft Internet Explorer is prone to a heap buffer overflow vulnerability. The vulnerability arises because of the way Internet Explorer tries to instantiate certain COM objects as ActiveX controls. An attacker can exploit this issue to execute arbitrary code within context of the affected application. Failed exploit attempts will result in a denial-of-service.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/19738/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/19738/references>

40. *August 28, Websense Security Labs* — **Malicious Website / Malicious Code: Microsoft Security Bulletin Scam.** Websense Security Labs has received reports of a new wave of e-mail scams disguised as Microsoft Security Bulletins. Users receive an e-mail message which urges the immediate installation of a cumulative security patch for the "plug and play" vulnerability. Upon visiting the site and running the code the user is infected with a password stealing Trojan horse.

Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=591>

Internet Alert Dashboard

Current Port Attacks	
Top 10	1026 (win-rpc), 4672 (eMule), 139 (netbios-ssn), 25 (smtp), 32794
Target	(---), 445 (microsoft-ds), 62641 (---), 113 (auth), 80 (www), 28561

Ports

(---)

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.